資料３

クレジットカードデータ利用に係る

API ガイドライン

事務局案（2017 年 12 月版）

2017 年 12 月 11 日

資料３

目次

青字部分は、「中間取りまとめ」より引用
赤字部分は、全銀協「オープン API のあり方に関する検討会報告書」より引用
黒字部分は、新たに追記等を行った箇所

1 はじめに

1.1 本ガイドラインの目的

クレジットカードに関連する様々な FinTech サービスが新たに生まれていくには、スクレイピングのような方法には一定の課題がある。こうした課題を解決する方法として、API によるカード会社と FinTech 企業等との連携が重要な鍵を握ると考えられる。

前述のスクレイピングと比べると、API 連携は契約締結等をした者にシステムへのアクセスを許諾するため、アクセスの正当性が明確化されることによる安全面の向上の他、アクセスされる側のシステムの負荷軽減、FinTech 企業等が利用者のログイン用 ID・PW を取得・保有することが不要になることによる FinTech 企業等における情報漏えいリスクの軽減という観点から優れているとの指摘がある。よりセキュアな API 連携でデータ取得を行うことは、FinTech 企業等にとってもデータの同期速度が安定・迅速化する。実際、家計簿サービスにおいて、銀行口座のデータを取得する際に API 連携を行っている事例があり、その銀行を利用するユーザーの一部から、情報取得の失敗頻度が減ったといった評価を受けている。

また、新しいサービスを開発しようとする時、自社の限られたリソースによる自前主義の開発の場合は迅速性に限界があるが、カード会社が API を用意すれば、それを連携先に提供し、連携先がそれに合わせて開発することになるため、カード会社側の開発負担は削減されることとなり、開発時間も短縮化するとともに、連携先数の飛躍的増加が可能となる。

このように、API 連携はカード会社と FinTech 企業等が連携を行う上で様々なメリットがある連携手段である。

また、第４次産業革命が進展し、データの処理技術や分析技術が高度化する中で、カード会社や FinTech 企業等の異なる主体が保有するデータを円滑に融通できるようにし、クレジットカードデータの情報としての社会的価値を最大化することが求められる。この観点からも、カード会社と FinTech 企業等による API 連携を更に促進することは重要である。

本ガイドラインは、今後、クレジットカード会社（以下、「カード会社」）と FinTech 企業を始めとする外部企業との多対多の API 連携が想定される中、API 仕様、セキュリティ及び利用者保護の対策について、規範としての方向性を示すことで、API 連携に係る事業者各位におけるサービス提供の効率化、オープン・イノベーションの促進、及び安心・安全な利用環境の創出を目指すことを目的としている。

また、本ガイドラインを策定することで、カード会社単独でサービス提供することに加え、カード会社が API 連携によって FinTech 企業等を活用することで、クレジットカード

青字部分は、「中間取りまとめ」より引用
赤字部分は、全銀協「オープン API のあり方に関する検討会報告書」より引用
黒字部分は、新たに追記等を行った箇所

に関する今までに無かったような新しいサービスが創出され普及することにより、カードサービスの利便性が一層向上するとともに、ひいては更なるキャッシュレス決済の普及に繋がっていくことを目指す。

本ガイドラインは、カード会社、FinTech 企業、小売業者、業界有識者、弁護士等の幅広い関係者による議論の結果として取りまとめられたものであり、本ガイドラインに基づいた、個別具体的なオープン・イノベーションの取組が行われることが期待される。

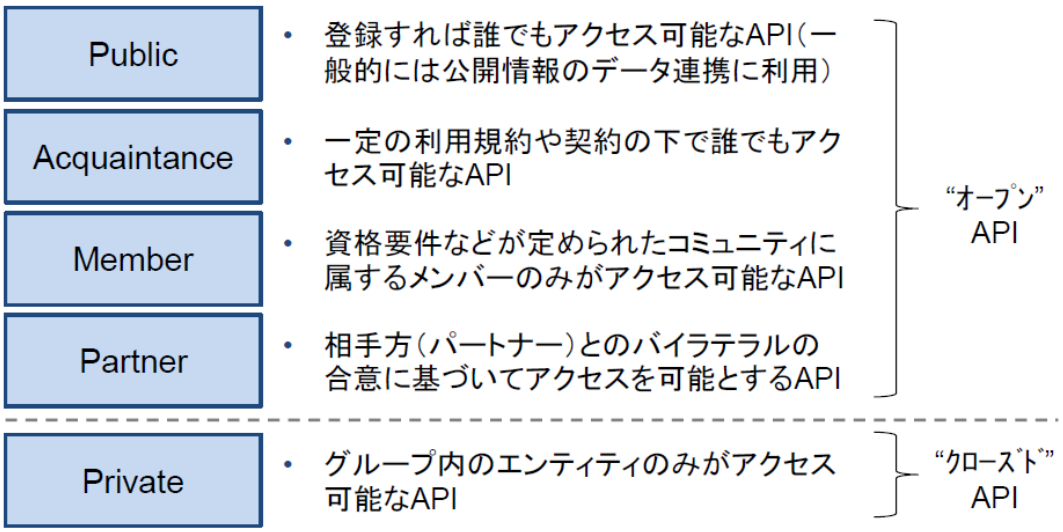
1.2 本ガイドラインの適用範囲

- オープン API の適用範囲として、本ガイドラインでは、開放性、業務、機能の３つの分類について規定する。
- 本ガイドラインは、1.1 本ガイドラインの目的 にて示したように、クレジットカード業務においてオープン API を導入する際の規範であり、必ずしもカード会社に対し、API の開放をその意に反して要求するものではない。

（１） オープン API の開放性

- オープン API の開放性には、その開放の度合いに応じて、一般的に以下の４つの類型が想定される。本ガイドラインは、この４つの類型全てについて適用対象とする。

図表 1 オープン API の開放性に関する類型



（出典）Euro Banking Association “Understanding the business relevance of Open APIs and Open Banking for banks”, May 2016 を基に NTT データ経営研究所作成

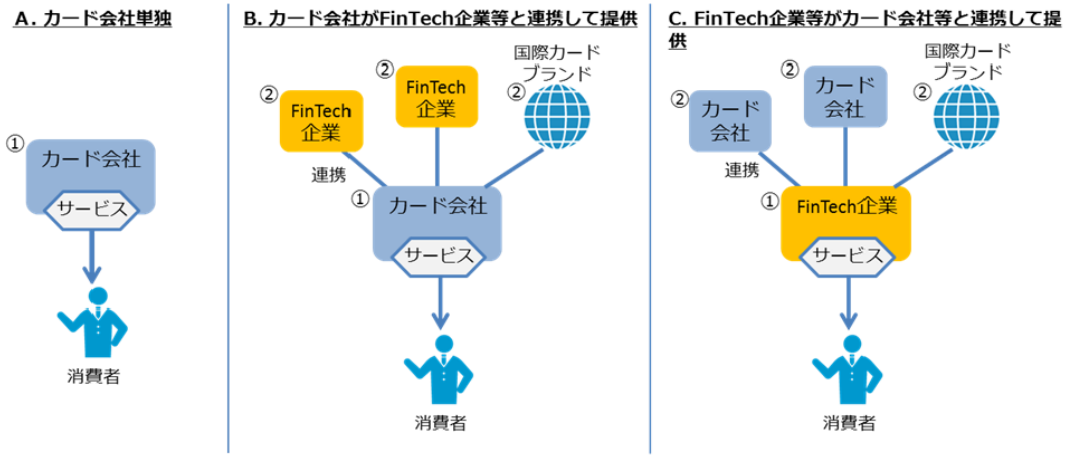
青字部分は、「中間取りまとめ」より引用
赤字部分は、全銀協「オープン API のあり方に関する検討会報告書」より引用
黒字部分は、新たに追記等を行った箇所

（２） 対象業務

i. API 関連事業者の立ち位置

- サービスが提供される上で、事業者の立ち位置として、消費者との接点を持つサービス提供者（①）と、そのサービスの実現に必要な技術や情報をサービス提供者に提供する事業者（②）の２つが考えられる。具体的な事業者として、カード会社、国際カードブランド、それ以外の FinTech 企業等を想定すると、このうち国際カードブランドは、サービス提供者をサポートする立ち位置をとっている(②に相当)。
- サービスの提供形態をパターン分けをすると、A.カード会社単独での提供、B.カード会社が FinTech 企業等外部企業と連携して提供する形、C.FinTech 企業等がカード会社等と連携して提供する形の 3 パターンが主に考えられる。

図表 2 クレジットカードに関するサービス提供形態



（出典）クレジットカード利用に係る API 連携に関する検討会「中間取りまとめ」（平成 29 年 6 月）

- なお、本ガイドラインで言う消費者とは、個人である消費者だけでなく、例えばクラウド会計サービスを利用する法人カードを利用する法人も含まれる。

ii. PAN 情報及び ID/パスワードの API 不通過

- クレジットカード業務では、PAN（Primarily Account Number）と呼ばれる、クレジットカードを一意に特定する番号が用いられる。この PAN 情報が漏えいすると、クレジットカードの不正利用に繋がることが容易に想定される。そのため、クレジットカード業界では PCI-DSS[1]等の非常に高度なセキュリティ体制を敷いていいる。
- API の活用において、この PAN 情報が取り扱われる場合、API 利用者である FinTech 企業等も PCI-DSS に準拠する必要が生じるほか、クレジットカード会社においても外

[1] Payment Card Industry Data Security Standard の略。クレジットカードの主要なブランド 5 社により設立された PCI SSC (Payment Card Industry Security Standards Council) が制定するクレジットカードに関するセキュリティ基準

部への流出を防ぐためのさらなる対策が求められることになる。

- また、クレジットカード会社が提供している Web サービス等で利用される ID 及びパスワードについては、消費者及びクレジットカード会社のみが把握し、API 利用者であったとしても不必要な保持は望ましくない。
- そのため、本ガイドラインで定める API に関する各規約は、PAN 情報及び ID/パスワードを取り扱わない前提として記載する。

（３） 対象機能

- カード会社に係る機能は、「参照系」「更新系」「認証系」の大きく三つに分類できる。
- 「参照系」とは、消費者の依頼に基づき、FinTech 企業等が、カード会社が保有する各種データを取得し、消費者に提供する業務を指す。この場合、取得したデータを FinTech 企業等が独自の加工をし、消費者へ提供する業務も含む。
- 「更新系」とは、消費者の依頼に基づき、FinTech 企業等が、カード会社の保有するデータについて、生成、更新、削除を必要とする依頼を行う業務を指す。
- 「認証系」とは、消費者の依頼に基づき、FinTech 企業等が、カード会社が保有する、消費者を識別するための情報を取得する業務を指す。
- 本ガイドラインでは、現時点でニーズが高く、サービスの具体化が想定されるイシュアにおける「参照系」（特に、PFM サービスや会計ソフト等における利用明細の照会）について定めるものである。なお、「更新系」「認証系」については、その利用を妨げるものではない。

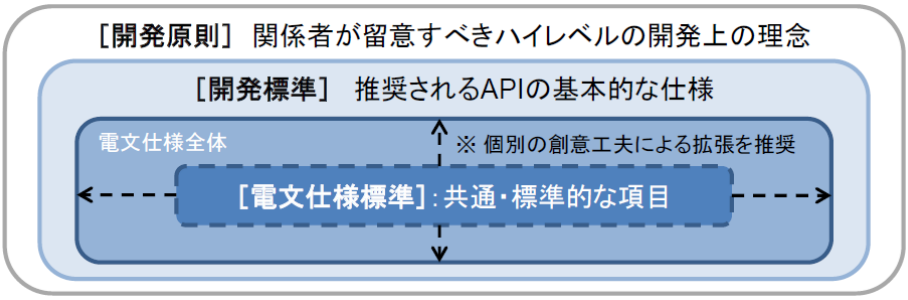
青字部分は、「中間取りまとめ」より引用
赤字部分は、全銀協「オープン API のあり方に関する検討会報告書」より引用
黒字部分は、新たに追記等を行った箇所

2 API 仕様の標準化

2.1 基本的な考え方

- API の仕様は、セキュリティ水準の確保、利用者保護の実現、及びカード会社と FinTech 企業等の協働・連携を通じたオープン・イノベーションの促進を図るうえでも、重要な論点である。
- システム連携を行うための対応作業、特に開発面における作業において、API 仕様のガイドラインがあれば、カード会社は API を開発しやすく、API 接続を行う FinTech 企業等もカード会社の API が出来るだけ統一されていると、開発負担が軽減される。
- 金融機関における API 仕様の標準化については、前述の「オープン API のあり方に関する検討会」において、開発原則、開発標準、電文仕様標準の 3 段階で議論されてきた。電文仕様標準についても「残高照会」及び「入出金取引明細紹介」の二つの機能について定められている。

図表 3 開発原則、開発標準、電文仕様標準の関係



（出典）オープン API のあり方に関する検討会「オープン API のあり方に関する検討会報告書 ― オープン・イノベーションの活性化に向けて ―」（2017 年 7 月 13 日）

- しかしながら、金融機関の「残高照会」及び「入出金取引明細紹介」の各機能に比べ、カード会社が提供する機能に関するデータは、各カード会社独自の仕様に基づき設計されており、乖離も大きい。個々のカード会社と FinTech 企業等とが個別に協業・連携して検討する革新的なサービスを含め、その全てに対応する標準仕様を定めることは困難かつ適当ではなく、電文仕様の標準化に向けた業界内の合意形成に相当の時間を要することが想定される。
- オープン・イノベーションの実現において、スピードは重要であり、業界内の合意形成を待ってガイドラインを作成することは、かえってオープン・イノベーションを阻害することになりかねない。

青字部分は、「中間取りまとめ」より引用
赤字部分は、全銀協「オープン API のあり方に関する検討会報告書」より引用
黒字部分は、新たに追記等を行った箇所

- 上記の判断より、現時点での電文仕様標準化は行わず、開発原則、開発標準についてのみ規定することとする。

2.2 開発原則

（１） 開発原則の目的と位置付け

- 「開発原則」は、関係者が API を開発・仕様決定するに当たり、留意すべきハイレベルの開発上の理念を定めるものである。
- オープン API は、カード会社システムへの接続仕様等を他の事業者等に公開するものであり、基本的にカード会社のみがユーザーとなる既存のカード会社システムと異なり、API の種類に拘らず、ユーザーとなる他の事業者等を意識したオープンな設計思想が求められる。
- 「開発原則」は、かかる観点から、関係者が API を開発・仕様決定するに当たり、留意すべき開発上の理念を示すことで、オープン・イノベーションが醸成されやすい環境の実現を後押しすることを目的としている。

（２） 開発原則

【原則1】API 利用者目線を意識した分かりやすくシンプルな設計・記述とすること

- オープン API は、他の事業者等による利用を前提とするものであり、API 利用者目線を意識したわかりやすくシンプルな設計・記述とすることが求められる。かかる設計・記述は、API 利用者側でのバグの発生リスクの抑制や複数カード会社と接続する FinTech サービスにおけるカード会社間の仕様差異の調整の容易化、カード会社が他の事業者等と連携する際の API の汎用性、拡張性の確保にも資する。
- 設計・記述に当たっては、API 接続候補先等の事業者等ともよく協議・連携することが望ましい。また、API の仕様決定後は、接続相手方が関係する部分の仕様について自社特有の用語やクレジットカード業界特有の略語等を使用しない平易な解説書（仕様書）を準備する等によって、API の仕様に対する接続相手方の誤解・誤認等を防止することが推奨される。
- シンプルな設計・記述とすることは、実際のサービスに必要な項目のみを抽出のうえ提供する等の対応を意味し、メッセージ上の項目数の削減のみを目的に種類・性質の異なる複数の項目を結合・統合する等の対応を意味しない。一般に、統合された項目を分離して接続相手方がシステムに取り込むよりも、分離された項目を接続相手方において統合する方が、接続相手方のシステム設計がシンプルかつ汎用性の高いものとなる。

【原則2】API の種類に応じた適切なセキュリティレベルを確保すること

- クレジットカード API では、カード会社の保有する秘匿性の高い情報が提供されるた

め、API の種類に応じた適切なセキュリティレベルを確保することが必要である。認証方式、通信方式等を含めた、具体的なセキュリティ対策やその水準については、「3 セキュリティ対策及び利用者保護対策」を参照のこと。

- セキュリティレベルを確保するうえでは、提供する各 API のスコープ（機能）を適切な粒度とし、接続相手方が認可された権限以上の API を使用できないようにすることが必要である。
- サイバー攻撃やサイバー犯罪の手口は年々巧妙化しているため、API のセキュリティ対策および水準は、接続相手方とも連携のうえ、継続的な改善・見直し、高度化を図っていくことが必要である。
- API の仕様書を一般に公開する場合、セキュリティに及ぼす影響について留意することが必要である。

【原則3】デファクトスタンダードや諸外国の API 標準、国際標準規格との整合性を意識すること

- 参照可能な国際標準規格等が存在する場合は可能な限り使用することが推奨される。例えば、日付や時刻の表現形式には RFC3339 や ISO8601/JISX0301、通貨コードの表現形式には ISO4217 といった標準がある。
- アーキテクチャ・スタイルやデータ表現形式、認可プロトコル等の仕様については、デファクトスタンダードや諸外国の API 標準、国際標準規格等との整合性を踏まえ、「2.3 開発標準」において推奨される基本的な仕様を定めている。

【原則4】仕様変更による API 利用者への影響をコントロールすること

- API の仕様変更は、ユーザーである接続相手方でもプログラム変更等の影響が生じることから、影響を適切にコントロールすることが必要である。クレジットカード API は、消費者の購買行動や資産管理行動の一部として機能する可能性があるため、仕様変更によって接続相手方が突然接続不能となった場合、接続相手方のサービスを利用する多くの利用者に影響・混乱が生じるおそれがある。
- 仕様変更による接続相手方への影響を抑制するため、API は、予めできるだけ汎用性、拡張性の高い設計とし、また、仕様変更が発生する可能性（機能追加、停止、バグ修正、データ形式の変更等）をできるだけ予め考慮した設計とすることが望ましい。これらは、各カード会社における API の仕様変更コストを低減することにも資する。
- 一方的な仕様変更によって接続相手方に混乱が生じないよう、仕様変更に当たっては、原則として十分な余裕をもって事前のアナウンスを行うことが必要である。また、新バージョン移行後も新旧バージョンを一定期間並行稼働させる、旧仕様を包含した新バージョンをリリースする等の対応も推奨される。
- パートナー型のオープン API の場合、通常、カード会社側から API 連携先を特定することが可能であるため、事前アナウンス等は比較的容易であるが、公開情報等をパブ

リック型のオープン API を通じて提供する場合等では、カード会社側から API 利用者を特定できない場合がある。また、パートナー型のオープン API であっても、カード会社への通知なく API の連鎖を許容している場合は、仕様変更の影響範囲をカード会社側で十分把握できない場合がある。このため、仕様変更に当たっては、影響範囲を十分慎重に見極めたうえで進めることが重要である。

- 推奨される具体的なバージョン管理の方法については、「2.3 開発標準」において定めている。

2.3 開発標準

（１） 開発標準の目的と位置付け

- 「開発標準」は、推奨される API の基本的な仕様を定めるものである。具体的には、①アーキテクチャ・スタイル、②データ表現形式、③認可プロトコル、④バージョン管理の四点について推奨される仕様を示す。
- 「開発標準」は、関係者が API の基本的な仕様を選択する際の目安となり、仕様の乱立による社会的コストを低減し、オープン・イノベーションが醸成されやすい環境の実現を後押しすることを目的としている。
- 「開発標準」への準拠は、各カード会社において検討・判断される。接続相手方との協議やサービスの特性等に応じて、親和性の高い適切な仕様が選択されることが重要である。
- 「開発標準」において推奨される基本的な仕様は、「2.2 開発原則」にもとづいて、諸外国を含めた API 利用者から支持されている仕様や、諸外国における標準（例：英国 Open Banking Standard）等との整合性を踏まえて定められている。
- 本ガイドラインは、「開発標準」が将来的な技術革新等に伴って陳腐化するリスクについても認識している。「開発標準」は、今後の技術革新の動向を踏まえ、必要に応じて見直すこととする。
- 「開発標準」は、各カード会社における、推奨された仕様以外の先進的な仕様や技術の採用を妨げるものではない。特に、セキュリティに関連する仕様については、より強固なセキュリティ水準を確保可能な最新の仕様があれば、同仕様を採用することが推奨される。

（２） 開発標準

i. アーキテクチャ・スタイル

- 「アーキテクチャ・スタイル」として、REST[2]を、「通信プロトコル」には HTTPs の

[2] Representational State Transfer の略。ソフトウェアがデータを連携するための設計原則の一つ。

使用を推奨する。REST は、Richardson Maturity Model [3] Level2（GET/POST/PUT/DELETE 等の HTTP 動詞の導入）を充足する設計とすることを推奨する。

ii. データ表現形式

- 「データ表現形式」として、JSON[4]を推奨する。

iii. 認可プロトコル

- 「認可プロトコル」として、OAuth2.0（RFC 6749）認可フレームワーク（以下「OAuth2.0」という。）を基本とする。
- また、より安全なトークンの授受を実現するため、PKCE（Proof Key for Code Exchange）(RFC 7636) の活用を推奨する。

iv. バージョン管理

- 「バージョン管理」として、セマンティック・バージョニングを推奨する。仕様変更による API 利用者への影響をコントロールする観点から、メジャー、マイナー、パッチ等の区分を用いて仕様変更レベルを管理する。

2.4 ステークホルダーの意見

2.5 その他期待される取組

[3] https://martinfowler.com/articles/richardsonMaturityModel.html を参照。
[4] JavaScript Object Notation の略。RFC7159 で規定される軽量なデータ記述言語。

青字部分は、「中間取りまとめ」より引用
赤字部分は、全銀協「オープン API のあり方に関する検討会報告書」より引用
黒字部分は、新たに追記等を行った箇所

3 セキュリティ対策及び利用者保護対策

3.1 基本的な考え方

- クレジットカード分野におけるオープン API の活用は、現在、世界的にも試行錯誤フェーズにあり、考え方の整理が必要な論点が多い。とりわけ、セキュリティ対策、利用者保護は、オープン API を活用したサービスに対する利用者の信頼を確保し、オープン API の普及、活用促進・円滑化を図るうえで、重要な論点である。
- オープン API では、利用者からの申請・同意にもとづいて行われるとはいえ、クレジットカード会社が保有する秘匿性の高い顧客情報が FinTech 企業等の他の事業者等（以下「API 接続先」という。）に提供され当該 API 接続先において蓄積・保存されることになる。それゆえ、オープン API に取り組むに当たっては、関係者において十分なセキュリティ対策、利用者保護が図られることが必要となる。
- 他方、API 接続先に対して、クレジットカード会社と同水準のセキュリティ対策、利用者保護策を徒に求めれば、API 接続先とクレジットカード会社の協働・連携による利便性の高い革新的なサービスの提供やサービスの高度化、イノベーションに向けた取組みが阻害され、利用者がテクノロジーの進展の恩恵を受ける機会を失うおそれがある。
- こうした認識の下、本ガイドラインでは、API の機能や連携するデータの種類・秘匿性等に応じたリスクベース・アプローチにもとづいて、利用者利便と利用者保護のバランスを踏まえた、クレジットカード分野のオープン API（クレカ API）におけるセキュリティ対策および利用者保護に関する基本的な考え方を取りまとめた。
- 取りまとめに当たっては、イノベーションを阻害しないよう留意するとともに、クレジットカード会社、API 接続先双方に対して対応水準の目安を示すことで、クレジットカード会社による API 接続先に対する過度に保守的なセキュリティ対策の要求や、セキュリティ上の懸念から生じるクレジットカード会社側のオープン API への取組みに対する躊躇といった課題を解消し、クレジットカード会社と FinTech 企業等の協業・連携の円滑化に資するものとすることを意識した。
- なお、先述のとおり、オープン API は、オープン・イノベーションを実現していくためのキー・テクノロジーの一つであり、今後、本技術を活用して、様々なビジネスモデルやサービスが提供されることが期待される。それゆえ、ビジネスモデルやサービスによって異なるリスクと対策の全てを網羅的に検討することは困難であり、本ガイドラインでは、様々なビジネスモデルやサービスに共通すると思われる主なリスクに対応したセキュリティ対策および利用者保護策に焦点をあてて取りまとめている。
- 具体的なセキュリティ対策および利用者保護策については、各クレジットカード会社

のポリシーや、個別のビジネス、各サービスのリスク、API 接続先の態様等に応じて個々に判断されるものであり、利用者保護の観点から、関係当事者において本ガイドラインの趣旨を十分に踏まえつつ、検討されることを期待する。例えば、リスクの内容等を勘案して本ガイドラインでは挙げていない追加的な対策を講じることも考えられる。他方で、リスクが小さいと考えられるビジネスやサービス等についてはセキュリティ対策を軽減することも考えられる。

- 以下では、オープン API において想定される主なリスクを整理したうえで、セキュリティ原則および利用者保護原則を示す。

3.2 オープン API の主なリスク

- オープン API では、クレジットカード会社のシステムに新たな通信路を設けて他の企業等を経由した新たなサービスを利用者（消費者）に提供することになるため、当該通信路を悪用したデータの漏洩・改竄や不正取引等が生じるリスクがある。
- 他方、クレジットカード会社や FinTech 企業等では、取扱うデータの重要性に鑑み、十分なセキュリティ対策や利用者保護対策を行ってきているのも事実である。
- そこで、本章ではオープン API に関するリスクを包括的に概観した後、オープン API の利用に伴い、新たに生じることが想定されるリスクに着目し、整理を行う。

（１） セキュリティ上のリスク

- API の利用に伴うセキュリティリスクを、下記の観点から分類した。実際に発生するリスクの発現は、これら観点に基づく要素の組合せによると言える。

i. リスクの発生要素に関する分類

a） 発生場所

- 発生場所は、「内部環境」と「外部環境」に分類できる。
- 内部環境とは、FinTech 企業やクレジットカード会社等の API 利用を行う企業、団体等（以下、「API 関係企業」）が直接的に管理下におくことのできる環境を指す。具体例として、API 関係企業の拠点、システム、ネットワーク、契約上管理下に置くことのできる外部システム、ネットワークを指す。
- 外部環境とは、API 関係企業の管理下にはない場所を指す。具体的には、公衆ネットワーク、スマートフォン等の利用顧客の有する環境、利用顧客等の生活環境、委託先の拠点、システム、ネットワークを指す。

b） 発生者

- 発生者は、「内部者」と「外部者」に分類できる。
- 内部者とは、上記の内部環境に直接的にアクセスできる者を指す。具体的には、API 関係企業の役職員や外部委託先の役職員を指す。

- 外部者とは、内部環境に直接的にアクセスできない者を指す。利用顧客や無関係の第三者が想定される。

c） 動機

- 動機は、「故意的」か「偶発的」かに分類できる。

d） 対象資産

- リスク発生時に対象となる資産は、「資金」「データ」及び「その他有形/無形」資産に分類できる。
- 資金には、顧客資金だけではなく、API 関係企業の資金も含む。
- データとは、API 関係企業の企業情報や利用顧客の個人情報に加え、システム上の設定値等が含まれる。

ii. API 利用に特有のリスク

- API の利用に伴うセキュリティリスクは、上述の通り、多様な要素の掛け合わせとなるため、多種多様であると言える。
- しかしながら、クレジットカード会社を始めとする API 関係企業では、従前よりリスク対策を行ってきていることも事実である。そのため、いたずらにリスクを指摘することは、既存の対策と重複した、さらなるセキュリティ対策コストを要求することとなり、かえってイノベーションを阻害する要因となりかねない。
- そのため、本ガイドラインでは、上記分類から導出される多様なセキュリティリスクの内、API 利用に特有のリスクについてのみ記載を行うこととする。当然ながら、他のリスクについても十分な対策が既にとられていることが前提となる。

a） API 基盤に関するセキュリティリスク

- API 基盤とは、API 接続を実現するためのシステム基盤を指す。当該基盤が独立して存在するか、他のシステムに内包されているかは問わない。
- API 基盤は、システムを管理する企業の外部へのゲートウェイとしての役割を担っており、不特定多数のアクセスが発生することが想定される。そのため、不特定多数のアクセスが発生することを想定したセキュリティ対応が求められる。システムへの侵入だけでなく、DDoS 攻撃等の大量データ送信による攻撃リスクも想定される。
- また、API 基盤における影響が、内部システムへ波及することによるリスクも想定される。

b） 公衆ネットワークにおける API 通信に関するセキュリティリスク

- API 通信は、インターネット等の公衆ネットワークを介して行われることが想定される。そのため、悪意のある第三者により、通信内容の傍受、改ざん、消去等が行われるリスクが内在する。
- この公衆ネットワークの利用は、消費者－FinTech 企業等間、及び FinTech 企業等－

クレジットカード会社間の 2 経路があり、双方におけるリスクを考慮する必要がある。

c） トークン管理に関するセキュリティリスク

- 「2.3 開発標準」において記載したとおり、認可プロトコルでは OAuth2.0 の利用が推奨される。本プロトコルはトークンを利用した認可処理が行われる。そのため、トークンを発行するクレジットカード会社、トークンを利用する FinTech 企業等の双方において、トークンの管理に対するセキュリティ対策が重要である。
- API 関係企業において、トークンの流出、偽造のリスクを考慮する必要がある。

（２） 利用者保護上のリスク

- API 利用サービスは、その技術的特性から、下記の特徴が挙げられる。
  - 不特定多数の消費者が利用する
  - サービス提供の基礎となる API を始めとする技術要件が一般消費者にとって高度かつ複雑であり、十分な理解を得ることが困難である
  - スマートフォンのアプリ等による対面でのサービス提供が行われない
  - 本来のサービス提供者（クレジットカード会社）と、直接のサービス提供者（FinTech 企業等）が異なる
- 上記の特徴から、消費者がサービス提供主体、提供内容等を十分に理解しないままサービスを利用するというリスクが内在する。
- また、消費者に発生した損害に対する補償が十分に得られないというリスクも存在する。
- 消費者が理解してサービスを利用する、いわゆる「インフォームド・コンセント」の考え方が求められる。

3.3 セキュリティ原則

（１） API 接続先の適格性

i. 事前審査

- クレジットカード会社は、FinTech 企業等との API 接続に先立ち、セキュリティ等の観点から、API 接続先の適格性を審査することが必要である[5]。
- セキュリティに関連した適格性の審査に当たっては、少なくとも以下の点について API 接続先に確認することが必要である[6]。
  - セキュリティ原則の充足状況
  - 過去に発生したセキュリティ関連の不祥事案と改善状況

[5] 情報セキュリティ以外の適格性については、「3.4 利用者保護原則」を参照。
[6] API 接続先が ASP やクラウドサービスを利用している場合には、API 接続先から必要な開示が行われる必要があることに留意する

青字部分は、「中間取りまとめ」より引用
赤字部分は、全銀協「オープン API のあり方に関する検討会報告書」より引用
黒字部分は、新たに追記等を行った箇所

- 利用者の属性や取引のリスクに応じた、継続的なセキュリティ対策の高度化に向けた態勢やリソースの有無

- 適格性の審査は、画一的・機械的に行うものではなく、また、上記に限らず、各企業等との API 接続によって目指すビジネスモデルやその固有リスク、各銀行のセキュリティポリシー等に応じて、各クレジットカード会社が独自に必要と判断した事項も加えて実施する必要がある。
- なお、API 接続先が任意に定めたセキュリティポリシーやセキュリティ関連文書、API 接続先が取得した情報セキュリティ関連の認証（ISO27001、TRUSTe、等）、銀行との API 接続状況等は、上記の適格性の審査に当たっての参考になると考えられる。
- 複数のクレジットカード会社と API 接続する企業等における審査対応負担を軽減する観点から、情報セキュリティ関連機関において、クレジットカード会社が API 接続先の適格性を審査する際に使用する、必須確認項目と独自確認項目からなる「API 接続先チェックリスト」（仮称）を制定することが期待される[7]。
- なお、事前審査は、各クレジットカード会社がそれぞれ独立に行うことを前提としつつも、複数のクレジットカード会社と API 接続する企業等における審査対応負担の軽減やクレジットカード会社による事前審査水準の標準化の観点から、当該クレジットカード会社の責任において他のクレジットカード会社に事前審査を委ねたり、他のクレジットカード会社が既に行った事前審査の結果を参考にしたりすることも考えられる[8]。

ii. モニタリング

- クレジットカード会社は、API 接続先の情報セキュリティに関連した適格性について、API 接続後も定期的にまたは必要に応じて確認することが必要である[9]。
- モニタリングの方法、深度、頻度等については、利用者の属性や取引のリスク、各企業等との API 接続によって目指すビジネスモデルやその固有リスク、各クレジットカード会社のセキュリティポリシー等に応じて、個別に判断されると考えられる。
- クレジットカード会社は、API 接続に当たって、API 接続先との間でモニタリングに関する事項（例：方法、深度、頻度、必要に応じた立入検査等、情報セキュリティ対策の大幅な変更を行う場合の対応、等）を予め取り決めておくことが必要である。
- クレジットカード会社は、API 接続先の情報セキュリティに関連した適格性に懸念があると判断した場合には、API 接続先に対して改善を求め、利用者保護の観点から、

---

[7] 必須確認項目については、却って API 接続先の対応負担が重くならないよう極力共通した内容に止めるとともに、投入人数や資本額等の形式面ではなく運用を含めた実質面に着目した確認を可能な内容とする等の留意が必要と考えられる。
[8] 本方式を採用する場合のクレジットカード会社間の取決めに係る留意点については、銀行会で検討が行われている「共同監査方式」の枠組みが参考になると考えられる。
[9] API 接続先が定期的な情報セキュリティ関連の外部監査を受けている場合には、それらの結果を活用すること等も考えられる。

必要な場合には API 接続先のアクセス権限の制限、停止、取消等を行わなければならない[10]。

- なお、モニタリングは、各クレジットカード会社がそれぞれ独立に行うことを前提としつつも、複数のクレジットカード会社と API 接続する企業等におけるモニタリング対応負担の軽減や、クレジットカード会社によるモニタリング水準の標準化の観点から、当該クレジットカード会社の責任において他のクレジットカード会社にモニタリングを委ねたり、他の銀行が既に行ったモニタリングの結果を参考にしたりすることも考えられる[11]。

（２） 外部からの不正アクセス対策

- 以下は、アクセス権限の認可に OAuth2.0 を実装したシステムを前提とした記載。なお、同等のまたはより強固な認可・認証が可能な他のプロトコル（新たなテクノロジーを含む）の採用を妨げるものではない。

i. （アクセス権限の付与に係る認証）

- クレジットカード会社は、公表情報または匿名加工情報を提供する場合を除き、API 接続先に対するアクセス権限の付与（OAuth2.0 においては「認可」）を利用者の申請にもとづき行うこととし、その際、利用者の本人認証を行わなければならない。
- 認証方式は、利用者の属性や付与するアクセス権限の内容とそのリスクに応じた強度とすることが必要である[12]。
- 認証方式の選択に当たっては、当該クレジットカード会社において採用されている他のオープンネットワークを利用した取引チャネル（例：Web サービス）の認証方式の水準が一つの目安となり得るが、以下の点にも留意が必要である。
  - 個々の取引に係る認証ではなく、アクセス権限の認可に係る認証であること
  - API を通じて指図を受ける個々の取引に係る認証方式も勘案した全体の不正アクセスリスクに応じた認証強度とする必要があること
- 当該クレジットカード会社において採用されている他のオープンネットワークを利用した取引チャネルの認証方式と比較して、強度の劣後する認証方式を採用する場合には、不正アクセスリスクが高まることを踏まえた利用者保護上の別途の対策が必要となる。例えば、店頭手続・郵送確認等を併用する、参照可能範囲を制限する、トークンの有効期限を短期とする、不正使用発生時の補償を予め定める、等が考えられる。

---

[10] ただし、クレジットカード会社が恣意的な判断によりアクセスを制限して API 接続先の事業に影響を与えることのないよう留意する。
[11] 本方式を採用する場合のクレジットカード会社間の取決めに係る留意点については、銀行会で検討が行われている「共同監査方式」の枠組みが参考になると考えられる。
[12] 各クレジットカード会社の判断にもとづき、利用者保護の観点から、強固な認証方式を一律に採用することも妨げない。

青字部分は、「中間取りまとめ」より引用
赤字部分は、全銀協「オープン API のあり方に関する検討会報告書」より引用
黒字部分は、新たに追記等を行った箇所

ii. アクセス権限／トークンの管理

- クレジットカード会社は、API 接続先に付与するアクセス権限（OAuth2.0 においては「トークン」が発行される）の管理について、以下の点に留意することが必要である。
  - 付与するアクセス権限は、API 接続先が提供するサービスに必要な範囲に限定すること（利用者からの申請／同意があったとしても、不必要なアクセス権限を API 接続先に付与しないこと）
  - API 接続先に発行するトークンには、利用者属性やアクセス権限の内容とそのリスク、利用者の利便性等を踏まえた適切な有効期限を設定すること
  - アクセス権限の内容に応じたトークンの偽造・盗用対策を講じること
  - 不正アクセス等を検知、または発生した場合に速やかにアクセス権限の制限、停止、取消が可能な仕組みとすること
- クレジットカード会社は、アクセス権限やトークンを管理するシステムに堅牢なセキュリティ対策を講じなければならない。また、API 接続先に対しても、トークンの適切な管理とセキュリティ対策を求めなければならない。

iii. 通信方式

- 通信方式としてオープンネットワークを使用する場合、第三者による盗取等を防止する観点から、TLS を使用して保護することが必要である。

iv. システムの堅牢性

- クレジットカード会社は、顧客情報について、商慣習または信義則にもとづく私法上の義務として守秘義務を負うほか、日本クレジット協会（JCA）の「カード情報の保護対策の計画」やクレジット取引セキュリティ対策協議会の「クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画」等を参考に、顧客の利益が不当に害されることのないよう当該業務に関する情報を適正に管理し、かつ当該業務の実施状況を適切に監視するための体制の整備その他必要な措置を講じることが求められる。
- クレジットカード会社が保有する顧客情報の秘匿性を踏まえれば、利用者保護や不正アクセス／情報流出防止の観点から、API 接続先（特に複数クレジットカード会社の大量の顧客情報を蓄積している PFM 事業者）においても、クレジットカード会社と同水準のセキュリティ対策が講じられることが理想的であるものの、クレジットカード業を前提とした上記安全管理措置を一律に API 接続先に適用することは必ずしも適当ではないと考えられる。また、クレジットカード会社が行っている外部委託先に対するシステムリスク管理の考え方についても参考になるものの、オープン API では、外部委託と異なり、クレジットカード会社から API 接続先への情報提供は利用者からの申請／同意にもとづくものであることや高い堅牢性が求められるクレジットカード会社システムの一部を外部委託するものではないことから、外部委託先管理の枠組みを

一律に適用できるわけではないと考えられる。

- API 接続先が確保すべき安全管理措置の水準は、API 接続先が取得・保有する情報の内容と量、情報が万一流出した場合に想定される利用者への影響や被害、API 接続先に対する利用者の情報管理に関する期待の程度等を踏まえて、第一義的には API 接続先が自らリスクベースで個別に判断することが必要である。
- API 接続先が確保すべき安全管理措置の目安水準については、最低限、API 接続先においても以下の措置は必要である。
  - ウィルス対策ソフトの導入
  - 機密性の高い情報（例：API 接続先の ID/PW やクライアント証明書、トークン、等）の暗号化
  - ファイアーウォール等のサイバー攻撃に対する多層防御の導入
  - サーバ変更監視（改竄検知）、ネットワーク監視
  - 公開サーバ脆弱性対策
  - API 実行ログ（ユーザー、操作、結果、等）取得、保管
  - 情報喪失等に備えたバックアップ等の対策
- なお、API 接続先に、顧客の同意を得て銀行が提供する個人情報（個人データ）の個人情報保護法上の取扱いは、個別のスキームに応じて個々に判断されるべきものではあるが、原則的にはクレジットカード会社は API 接続先に対して、個人情報委託先の監督義務（同法第 22 条）を負っていないと解するのが適当と考えられる。

v. 不正検知・監視機能

- 不正検知・監視機能は、不正アクセス被害の発生やその拡大を未然に防止するうえで重要な機能の一つである。
- オープン API においては、利用者の IP アドレスや認証失敗回数等の不正検知に活用される情報をクレジットカード会社が直接入手できなくなるため、取引のリスクに応じて、クレジットカード会社が必要とする場合には、API 接続先から銀行に不正検知に必要な情報が提供される仕組みを構築することが必要である。
- API 接続先についても、API 接続先が取得・保有する情報の内容と量、当該情報が万一流出した場合に想定される利用者への影響や被害、API 接続先に対する利用者の情報管理に関する期待の程度等を踏まえて、情報セキュリティ関連機関において、不正検知・監視機能の要否やその水準等についての考え方や留意点の整理が行われることが期待される。

（３） 不正アクセス発生時の対応

i. システム設計・仕様

- クレジットカード会社および API 接続先は、不正アクセスが判明した場合に被害発生やその拡大を未然に防止する観点から、速やかに、クレジットカード会社においては

アクセス権限の制限、停止、取消を、API 接続先においてはサービス利用の制限、停止を行うことができるシステム設計・仕様としなければならない。

- クレジットカード会社および API 接続先は、不審なアクセス等についての利用者からの照会への対応や、不正アクセス発生時の原因調査、必要な対策の検討を行うため、適切なアクセスログの記録および保存を行わなければならない。

ii. 情報連携、対策協議

- 不正アクセス発生時には、速やかにクレジットカード会社と API 接続先の間で情報連携を行うとともに、原因調査や必要な対策の協議等を協力して行っていくことが必要である。必要な対応については、クレジットカード会社と API 接続先との間で予め取り決めて明確化しておくことが必要である。

（４） セキュリティ対策の継続的な改善・見直し、高度化

- サイバー攻撃やサイバー犯罪の手口は年々巧妙化しているうえ、オープン API を活用したサービス提供は世界的にみても現状、初期段階にある。そのため、クレジットカード会社および API 接続先は、自社のみならず他社での不正アクセス事例等を踏まえ、セキュリティ対策の継続的な改善・見直し、高度化を図っていくことが必要である。
- セキュリティ対策の改善・見直し、高度化に向けては、クレジットカード会社および API 接続先は、協力して取り組むことが重要と考えられる。

3.4 利用者保護原則

（１） API 接続先の適格性

i. 事前審査

- クレジットカード会社は、他の事業者等との API 接続に先立ち、利用者保護等の観点から、API 接続先の適格性を審査することが必要である[13]。なお、クレジットカード会社が共通システムを通じて API 接続先と接続する場合については、クレジットカード会社による API 接続先の審査結果にもとづき、共通システム提供事業者が API 接続先との接続を行うものとする。
- 適格性の審査に当たっては、少なくとも以下の点について API 接続先に確認することが必要である。
  - グループ会社を含めた事業内容、兼業内容
  - 反社会的勢力との関係の有無を含む社会的信用、組織ガバナンス
  - 法令遵守態勢

[13] 情報セキュリティ関連の適格性については、「3.3 セキュリティ原則」の「3.3.1 API 接続先の適格性」を参照。

青字部分は、「中間取りまとめ」より引用
赤字部分は、全銀協「オープン API のあり方に関する検討会報告書」より引用
黒字部分は、新たに追記等を行った箇所

- 利用者保護態勢[14]
- 利用者保護原則の充足状況
- 過去に発生した利用者保護関連の不祥事案と改善状況
- 利用者の属性や取引のリスクに応じた、継続的な利用者保護策の高度化に向けた態勢やリソースの有無

- 適格性の審査は、画一的・機械的に行うものではなく、また、上記に限らず、各企業等との API 接続によって目指すビジネスモデルやその固有リスク、各クレジットカード会社の顧客保護等管理規程等に応じて、各クレジットカード会社が独自に必要と判断した事項も加えて実施する必要がある。
- なお、API 接続先が定めた社内規定等は、上記の適格性の審査に当たっての参考になると考えられる。
- 複数のクレジットカード会社と API 接続する企業等における審査対応負担を軽減する観点から、情報セキュリティ関連機関において、クレジットカード会社が API 接続先の適格性を審査する際に使用する、必須確認項目と独自確認項目からなる「API 接続先チェックリスト」（仮称）を制定することが期待される。
- なお、事前審査は、各銀行がそれぞれ独立に行うことを前提としつつも、複数のクレジットカード会社と API 接続する企業等における審査対応負担の軽減やクレジットカード会社による事前審査水準の標準化の観点から、当該クレジットカード会社の責任において他のクレジットカード会社に事前審査を委ねたり、他の銀行が既に行った事前審査の結果を参考にしたりすることも考えられる[15]。適格性の審査に当たっては、少なくとも以下の点について API 接続先に確認することが必要である。

ii. モニタリング

- クレジットカード会社は、API 接続先の適格性について、API 接続後も定期的にまたは必要に応じて確認することが必要である。
- モニタリングの方法、深度、頻度等については、利用者の属性や取引のリスク、各企業等との API 接続によって目指すビジネスモデルやその固有リスク、各クレジットカード会社の顧客保護等管理規程等に応じて、個別に判断されると考えられる。
- クレジットカード会社は、API 接続に当たって、API 接続先との間でモニタリングに関する事項（例えば、方法、深度、頻度、API 接続先に提出を求める情報、API 接続先が大幅な態勢見直しや業務停止等を行う場合の対応、等）を予め取り決めておくことが必要である。
- クレジットカード会社は、API 接続先の利用者保護態勢等に関する適格性に懸念があ

[14] 特に顧客情報の適切な取扱い・管理態勢や、取得情報の利用目的の適切性、利用約款の適切性（過度な免責規定等、利用者保護に著しく欠ける条項の有無）について確認する。
[15] 本方式を採用する場合のクレジットカード会社間の取決めに係る留意点については、銀行会で検討が行われている「共同監査方式」の枠組みが参考になると考えられる。

ると判断した場合には API 接続先に対して改善を求め、利用者保護の観点から必要な場合には API 接続先のアクセス権限の制限、停止、取消等を行わなければならない[16]。

- なお、モニタリングは、各クレジットカード会社がそれぞれ独立に行うことを前提としつつも、複数のクレジットカード会社と API 接続する企業等におけるモニタリング対応負担の軽減や、クレジットカード会社によるモニタリング水準の標準化の観点から、当該クレジットカード会社の責任において他のクレジットカード会社にモニタリングを委ねたり、他のクレジットカード会社が既に行ったモニタリングの結果を参考にしたりすることも考えられる[17]。

iii. その他の留意点

- API 接続先において API 接続を通じて提供するサービスに関して利用者保護に欠ける不祥事案等が発生した場合、クレジットカード会社と API 接続先との関係、利用者からの見え方等によっては、クレジットカード会社側も社会的な批判を浴びる等のレピュテーションリスクが生じる可能性に留意が必要である。
- API 接続先が提供するサービスがクレジットカード会社の提供するサービス（例：Web サービス）を実質的に代替するものであって、かつクレジットカード会社側も自社サービスの提供を取り止めて、消費者に対して API 接続先のサービスの利用を推奨する場合は、形式上、クレジットカード会社と API 接続先の間に外部委託契約が締結されていなくとも、その実態において同視され、銀行法にもとづく外部委託規制の対象となる可能性があることに留意が必要である。
- API 接続先が提供するサービスがクレジットカード会社の提供するサービス（例：Web サービス）を実質的に代替するものであって、かつ利用者の大部分が当該 API 接続先のサービスの利用に依拠する場合は、API 接続先のシステム障害や業務停止等によって、利用者がサービスを利用できなくなり、混乱が生じるおそれがあることに留意が必要である。
- 事前の取決めにおいて、API 接続先における障害等によって銀行の業務に影響が生じるおそれがある場合には、ただちに銀行に連絡するよう定めておくことが必要である。なお、その他の障害等の報告要否やタイミングについても、予め取り決めておく必要があることに留意する。
- API 接続先もしくはクレジットカード会社の都合によるサービス停止を行う際は、一定期間の事前通知期間を設定することが必要である。

---

16 ただし、銀行が恣意的な判断によりアクセスを制限して API 接続先の事業に影響を与えることのないよう留意する。

17 本方式を採用する場合のクレジットカード会社間の取決めに係る留意点については、銀行会で検討が行われている「共同監査方式」の枠組みが参考になると考えられる。

青字部分は、「中間取りまとめ」より引用
赤字部分は、全銀協「オープン API のあり方に関する検討会報告書」より引用
黒字部分は、新たに追記等を行った箇所

（２） 説明・表示、同意取得

i. 重要な情報の表示、同意取得

- インターネットを利用した取引は、基本的に画面に表示される情報にもとづいて利用者の判断・同意が行われ、また、必要な情報を表示しても、利用者が十分に確認せずに、手続きを進める可能性がある。
- そのため、クレジットカード会社および API 接続先は、利用者の判断・同意に必要な情報を単に提供・表示するに止まらず、わかりやすく画面表示するとともに、誤認・誤解を招く表現を避け、また、利用者に重要な判断・同意を求めるものについては注意喚起プロセスを設けることや、利用者のシステム操作による同意を求めること等、利用者保護に十分配慮した表示方法、画面構成とすることに努めなければならない。
- クレジットカード会社は、トークン発行に当たって、少なくとも以下の点について、わかりやすく画面表示のうえ、利用者の同意を求めることが必要である。
  - アクセス権限を付与する API 接続先の名称
  - API 連携するサービス等の名称
  - 付与する権限の内容・範囲
  - 付与する権限の有効期限[18]
  - 付与した権限の削除、解除方法
  - その他注意喚起が必要な事項

ii. （リスク等に関する表示）

- API 接続先は、提供するサービスに関して生じる主なリスクの適切な表示に努めなければならない。
- API 接続先は、サービス提供時間帯または停止時間帯、休日・休業等のサービス提供上の制約について適切な表示に努めなければならない。

iii. 利用者の誤認防止

- 以下の点については、特に利用者の誤認や誤解が生じるおそれがあることに留意し、適切に表示することに努めなければならない。
  - API 接続先が提供するサービスはクレジットカード会社が提供するサービスとは異なること
  - クレジットカード会社と API 接続先の関係、それぞれの役割
  - クレジットカード会社と API 接続先の画面の区別
- なお、クレジットカード会社は、API 接続先が虚偽または意図的に誤認を招く表示を行っていることが判明した場合には、API 接続先に対して是正を求め、利用者保護の観点から、必要な場合には API 接続先のアクセス権限の制限、停止、取消、関係当局

[18] リフレッシュトークンを発行する場合には同トークンによって延長される最大の有効期限。

への通報等の必要な措置を講じなければならない。

iv. その他の表示

- クレジットカード会社および API 接続先は、利用者からの相談・照会、苦情、問合せがあった場合の役割分担、業務フロー等を、予め取り決めておくことが必要である。
- クレジットカード会社および API 接続先は、上記の取決め内容を踏まえ、利用者からの相談・照会、苦情、問合せに対応するための連絡先を表示することが必要である。
- API 接続先は、商号、代表者、住所、連絡先等について表示することが必要である。
- API 接続先は、電磁的方法による決算公示を選択している場合、会社法にもとづく決算公告についても表示することが必要である。

（３） 不正アクセスの未然防止

- API 接続先は、不正アクセスを未然に防止する観点から、例えば以下の点について、利用者に注意喚起することに努めなければならない。
  - API 接続先のログインパスワード等は、クレジットカード会社サービスに利用しているパスワード等と異なるものを設定すること
  - API 接続先のログインパスワード等は、類推されやすいものを避けること、適切な管理に努め第三者に貸与、開示しないこと、定期的に変更すること
  - ウィルス対策ソフトを導入すること
- API 接続先は、利用者に対して、API 接続先のパスワード等の紛失、漏洩や不正アクセスの懸念がある場合には、ただちに API 接続先に対して連絡するよう求めておくことが必要である。

（４） 被害発生・拡大の未然防止

i. 初動対応

- クレジットカード会社または API 接続先において不正アクセス等が判明した場合、被害発生・拡大を未然に防止する観点から、速やかに、クレジットカード会社においてはアクセス権限の制限、停止、取消を、API 接続先においてはサービス利用の制限、停止を行うことが必要である。
- クレジットカード会社と API 接続先双方において速やかに機能制限、停止、その他必要な措置を行う観点から、一方で API に関連した不正アクセス、情報流出・漏洩が判明した場合にはただちに他方に連絡することとし、その場合の連絡先や連絡方法等を銀行と API 接続先間において予め取り決めておく等、被害拡大防止に向けた必要な態勢を整備しておくことが必要である。
- API 接続先が複数のクレジットカード会社と接続している場合において、他のクレジットカード会社においても同様の事案が発生するおそれがある場合には、API 接続先は当該他のクレジットカード会社に対してもただちに連絡し、被害拡大を未然に防止

することに努めなければならない。

ii. 利用者への連絡

- 被害が発生した利用者への連絡や、被害が広範な利用者に及ぶ可能性がある場合に利用者にただちに十分な注意喚起（例えば、ただちにパスワード等の変更を求める等）ができるよう、API 接続先は、利用者との連絡手段を予め確保しておくことが必要である。
- 利用者に届出・登録を求める連絡手段の範囲については、提供するサービスの内容や取引のリスクに応じて、個別に判断されると考えられる。
- クレジットカード会社は、API 接続先が利用者との十分な連絡手段を予め確保することができない場合、被害発生時に、銀行が API 接続先に代わって利用者に対し連絡、注意喚起する必要が生じる可能性に留意することが必要である。

（５） 利用者に対する責任・補償

- オープン API では、API 接続先とクレジットカード会社の双方が関与するため、情報流出やシステム上の不具合等により利用者に損害が発生した場合、利用者に対する責任の所在や、対応窓口・主体等が不明確になるおそれがある。
- 当事者の民事上の最終的な損害賠償責任を司法の判断に委ねた場合、速やかな被害回復、補償等が図られず、利用者保護に欠けるおそれがある[19]。

i. 当事者間における事前の取決め

- クレジットカード会社および API 接続先は、利用者に対して速やかな被害回復、補償等を図る観点から、不正アクセスや情報流出、不正送金、システム上の不具合等が発生した場合の対応窓口や、利用者に損害が生じた場合の補償・返金方法（含む、その主体）[20]、補償範囲について、予め取り決めておかなければならない[21]。なお、利用者に対して双方とも責任を負わない等の利用者保護に著しく欠ける取決めは、行ってはならない。
- API 接続先およびクレジットカード会社は、予め取り決めた利用者に対する補償・返金方法とその補償範囲（免責事由も含む）について、ウェブサイト等において利用者が常時確認できるよう表示するとともに、API 接続先が利用者と利用契約を締結する際にわかりやすく画面表示する等により、利用者が補償・返金を求める際の対応窓口やその方法について十分認識できるよう努めなければならない。

---

19 なお、本節における記述は、API 接続先およびクレジットカード会社が利用者保護の観点から自主的に行うことが期待される取組みであり、それぞれの利用者に対する最終的な法的責任を加重または軽減するものではない。

20 利用者への補償・返金後の、銀行と API 接続先の間の内部分担（求償）についても、別途予め取り決めておくことが望ましい。

21 クレジットカード会社および API 接続先が利用者に対して連帯して責任を負うこととする場合でも、利用者からみて対応窓口・主体等がわかりにくくなるおそれがあることから、任意の一次的な補償・返金方法（含む、その主体）等について、予め取り決めておくことが望ましい。

青字部分は、「中間取りまとめ」より引用
赤字部分は、全銀協「オープン API のあり方に関する検討会報告書」より引用
黒字部分は、新たに追記等を行った箇所

ii. 補償内容・範囲に関する考え方

- API を利用したサービスによる利用者の金銭的損害について、クレジットカード会社および API 接続先に過失がない場合でも、利用者が個人であって利用者自身の責任によらずに被害に遭われた場合については、上記事前の取決めにもとづいてクレジットカード会社または API 接続先から補償を行うことが必要である。なお、利用者に重大な過失または過失がある場合については、被害に遭った利用者の態様やその状況等を加味して、全額あるいは一部を利用者負担にすることも含め、個別に判断されることが必要である。
- 法人の利用者については、個人の利用者と比較して、セキュリティ対策等への対応力が相対的に高いと考えられる。利用者の利用環境やセキュリティレベルを原因として不正利用される可能性がある中では、サービス提供者側のセキュリティ対策に加え、利用者においてもセキュリティ対策を講じ、不正利用被害の防止に努めていくことが重要であると考えられる。こうした点を踏まえ、法人の利用者に対する補償については、利用者が行っていたセキュリティ対策や不正利用被害の防止に関する状況、法人の属性やセキュリティ対策への対応力等の点を考慮して、個別に判断されることが必要である。
- クレジットカード会社および API 接続先は、API を活用したサービスの形態や利用者の属性等に鑑みて、上記と異なる補償内容・範囲とすることに合理的な理由がある場合であって、かつ利用者に不測の損害が生じないよう、かかる補償内容・範囲について利用者に適切に説明または表示した場合に限り、補償内容・範囲を個別に定めることができる。

iii. API 接続先が補償・返金責任を負う場合の留意点

- クレジットカード会社と API 接続先との間の取決めにもとづき API 接続先が利用者に対して補償・返金責任を負う場合、クレジットカード会社は、API 接続先の利用者に対する補償・返金に係る態勢や資力等が利用者保護に欠けるおそれがないかに留意のうえ、API 接続の是非を判断するとともに、それらの状況について定期的にまたは必要に応じて確認することが必要である。
- クレジットカード会社は、API 接続先の補償・返金の態勢や資力等が利用者保護に欠けるおそれがあると判断した場合、API 接続先に対して態勢の見直しや責任財産の充実、責任保険への加入を求め、API 接続先においてそれが困難な場合は API 接続しない（あるいは接続の停止または取消を検討する）等の対応を行うことが必要である。
- API 接続先の利用約款等において API 接続先の免責事由が過大に定められている等（例えば、過失責任も負わない等[22]）、実質的に利用者に対する補償・返金責任が果たされ

[22] なお、事業者の債務不履行により消費者に生じた損害を賠償する責任の全部を免除する条項や、当該事業者、その代表者またはその使用する者の故意または重大な過失による事業者の債務不履行により消費者に生じた損害を賠償する責任の一部を免除する条項等は、消費者契約法（第 8 条乃至第 10 条）にもとづき

ないおそれがある場合、消費者契約法等を踏まえ、見直しを求めることが必要である。

3.5　その他

i.　公表情報の取扱い

- 店舗や提供するクレジットカードの種類等、クレジットカード会社のウェブサイト等においてログイン等の手続きを要さずに取得可能な公表情報（以下「公表情報」という。）を API 接続先に提供する場合は、上述の記載にかかわらず、以下の取扱いとすることが考えられる。
  - クレジットカード会社と API 接続先との通信経路において改竄が行われることを防止する観点から、銀行と API 接続先との通信方式は、セキュリティ原則「3.3（２） 外部からの不正アクセス対策」に定める通信方式に拠るものとする。
  - API 接続先は、システム上の不具合や外部または内部からの攻撃による改竄等によって、銀行に利用者からの問い合わせが行われる可能性のある事態が発生した場合には、ただちに関係銀行に対し連絡するよう努めなければならない
  - クレジットカード会社は、API の利用約款等において、不具合発生時等の責任について予め定めておくことが望ましい。
  - クレジットカード会社は、公表情報を提供する API のアクセス量をクレジットカード会社側でコントロールできない場合には、システムキャパシティの超過が原因で不具合が発生するリスクに留意するものとする。

ii.　「API 接続先の API 接続先」の取扱い

- クレジットカード会社は、API 接続先との間で「API 接続先の API 接続先」（以下「API 連鎖接続先[23]」という。）の取扱いについて予め取り決めておくことが必要である。
- これには、例えば、API 接続先と同様に取扱う（クレジットカード会社が API 連鎖接続先と直接契約を締結）、API の連鎖接続についてクレジットカード会社の承諾またはクレジットカード会社への事前通知を条件とする、連鎖接続を許容する条件を双方協議のうえ予め定める、API 接続先の責任と管理の下で連鎖接続を許容する等、様々な方法が考えられる[24]。
- いずれの方法による場合であっても、API 連鎖接続先において、本原則の趣旨を踏まえて、十分なセキュリティ対策と利用者保護が図られていることが重要である。
- なお、API 接続先が有する自社の情報を同接続先の API を通じて他の事業者等に提供することは、API の連鎖には該当しないが、個人情報保護法等にもとづき適切な利用

そもそも無効とされる。
[23] API 接続先がクレジットカード会社から取得した情報を、API 接続先と API 接続する他の事業者等が参照する場合における、当該他の事業者等をいう。
[24] API 連鎖接続先の取扱いは、例えば、取引のリスクに応じて参照系 API と更新系 API との間や、API 連鎖接続先が API 接続先と同一グループに属するか否かによって異なる取扱いとすることも考えられる。

青字部分は、「中間取りまとめ」より引用
赤字部分は、全銀協「オープン API のあり方に関する検討会報告書」より引用
黒字部分は、新たに追記等を行った箇所

者保護が図られる必要があることに留意する。